

Technische Ansätze für DSGVO-Transparenz

– Kurzvorstellung Projekt DaSKITA –

Dr.-Ing. Frank Pallas, TU Berlin, Information Systems Engineering
Digital Autonomy Hub Tutorial: Transparency Information Language

DaSKITA

Datensouveränität durch KI-basierte Transparenz und Auskunft

- „Datensouveränität durch KI-basierte Transparenz und Auskunft“
- Gefördert durch das Bundesministerium der Justiz und für Verbraucherschutz
- Partner:
 - TU Berlin, FG Information Systems Engineering
 - iRights.lab
 - <... weggefallen ...>
- 3 Jahre + 3 Monate (seit 01/2020)
- Diverse KI-basierte Ansätze zur Verbesserung der datenschutzrechtlichen „Informiertheit“ von Nutzer*innen in den Bereichen **Transparenz** und **Auskunft**

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, leicht verständlicher und leicht zugänglicher Form in einer für die betroffene Person verständlichen Sprache zu übermitteln; dies gilt insbesondere, wenn die Verarbeitung der personenbezogenen Daten automatisiert erfolgt. Wenn die betroffene Person Informationen erfolgt schriftlich oder über elektronische Kommunikationsmittel verlangt, kann die Information in derselben Form nachgewiesen wurde.

Artikel 15

Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

„Datensouveränität“ setzt ausreichendes Wissen & Verständnis der Verbraucher*innen voraus

→ Wer, was, wofür, wie lange, an wen, ...

→ Transparenz- und Auskunftspflichten in Art. 12ff DSGVO

„Transparenz“:

Nicht-individuelle Angaben, welche personenbezogenen Daten zu welchen Zwecken erhoben und verarbeitet, an welche Akteure sie weitergegeben, ... werden
(Art. 13/14)

„Auskunft“:

Individuelle Mitteilung über konkret vorliegende Inhaltsdaten zur anfragenden Person
(Art. 15, auch Art. 20 – „maschinenlesbares Format“)

Transparenzangaben “in the wild“

Hinweis zu ausgelagerten Dienstleistungen. Bestimmte Drittanbieter und Unternehmen der PayPal-Gruppe erbringen Dienstleistungen für PayPal (Europe) S.à r.l. et Cie, S.C.A. (PayPal), damit PayPal Ihnen Dienstleistungen anbieten kann. Wir geben möglicherweise Daten an diese Parteien weiter, darunter eventuell Kontoinformationen wie Ihre persönlichen und/oder geschäftlichen Angaben und Einzelheiten zu Ihren Transaktionen. Diese Drittanbieter haben ihren Sitz an verschiedenen Orten in der Europäischen Union (einschließlich Frankreich, Deutschland, Irland, Spanien, Niederlande, Bulgarien, Italien, Polen, Zypern, Schweden, Österreich und dem Vereinigten Königreich) sowie in Tunesien, Ägypten, El Salvador, den Philippinen und den Vereinigten Staaten. Gemäß dem Luxemburger Gesetz über den Finanzsektor haben wir diese Liste geändert, um die für solche Abbuchungen erforderlichen Daten zu berücksichtigen.

Kategorie	Name der Partei und Gerätezustand (in Klammern)	Zweck	Offenlegte Daten
1. Zahlungsbewerter	Barclays Bank Plc (GB), HSBC Bank Plc (GB, Irland), HSBC Merchant Services LLP (GB), Bank of America N.A. (EMEA, USA), BA Continuum India Private Limited (Indien), Discover Financial Services (USA), JPMorgan Chase Bank (GB, USA), BNP Paribas (Frankreich), Hergo (Schweden), Wells Fargo (Irland, USA), American Express (USA), National Westminster Bank Plc (GB), OmniPay Limited (Irland), Australia and New Zealand Banking Group Limited (Australien), ANZ National Bank Limited (Neuseeland), Transaction Network Services UK Limited (GB).	Zahlungsverarbeitung, Abwicklungsdienste und Betragsüberprüfung.	Name, Adresse, E-Mail-Adresse, Telefonnummer, Angaben zu Zahlungsquellen des Nutzers und Angaben zu Zahlungstransaktionen, Dokumentenaussweisnummer.
	BNP Paribas (Frankreich)	Zahlungsverarbeitung, Betragsüberprüfung und Konfliktbehandlung für Transaktionen von PayPal-Nutzern, wenn diese mit einem Händler zu tun haben, der den PayPal-Dienst über den BNP-Dienst nutzt.	Name, E-Mail-Adresse, Telefonnummer, Adresse, IP-Adresse, Geburtsdatum, PayPal-Kontonummer, Einzelheiten zu den Finanzierungsinstrumenten der Nutzer und Angaben zu Zahlungstransaktionen.
	VTB24 (Russland)	Zahlungsverarbeitung, Betragsüberprüfung und Konfliktbehandlung für Transaktionen von PayPal-Nutzern, wenn diese mit einem Händler zu tun haben, der den PayPal-Dienst über den VTB 24-Dienst nutzt.	Name, Adresse, E-Mail-Adresse, Telefonnummer, Angaben zu den Finanzierungsinstrumenten der Nutzer und weitere Angaben zu Zahlungstransaktionen.
	Deutsche Bank AG (Deutschland, Niederlande, Frankreich, Spanien)	Verarbeitung von Lastschriften in der SEPA-Region.	Name, Transaktionsdatum und -betrag, Währung und Bankverbindung des Nutzers.
	Royal Bank of Scotland plc (UK) ("RBS")	Zahlungsverarbeitung und Konfliktbehandlung für Transaktionen von PayPal-Nutzern, wenn diese mit einem Händler zu tun haben, der den	Alle Kontoinformationen außer Details zu Finanzierungsinstrumenten des Nutzers.

Welche Arten von Informationen erfassen wir?

Zur Bereitstellung der Facebook-Produkte müssen wir Informationen über dich verarbeiten. Die Arten der von uns erfassten Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, wie du auf von uns erfasste Informationen zugreifen bzw. sie löschen kannst, indem du die [Facebook-Einstellungen](#) bzw. die [Instagram-Einstellungen](#) besuchst.

Von dir und anderen getätigte und bereitgestellte Dinge.

- Von dir bereitgestellte Informationen und Inhalte.** Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt; dazu gehören auch deine Registrierung für ein Konto, das Erstellen oder Teilen von Inhalten sowie der Nachrichtenaustausch bzw. das Kommunizieren mit anderen. Dies kann Informationen über die von dir bereitgestellten Inhalte oder solche, die in ihnen enthalten sind (wie Metadaten) umfassen, wie z. B. den Aufnahme-Standort eines Fotos oder das Datum, an dem eine Datei erstellt wurde. Es kann auch das umfassen, was du durch von uns bereitgestellte Funktionen, wie z. B. unsere Kamera, siehst, damit wir dir beispielsweise Masken und Filter, die dir gefallen könnten, vorschlagen oder dir Tipps für die Verwendung des Hochformats geben können. Unsere Systeme verarbeiten von dir bereitgestellte Inhalte und Mitteilungen automatisch, um den Kontext und die in ihnen enthaltenen Details für die unten beschriebenen Zwecke zu analysieren. Erfahre mehr darüber, wie du kontrollieren kannst, wer die Dinge sehen kann, die du teilst.
- Daten mit besonderem Schutz.** Du kannst in deinen Facebook-Profilfeldern oder unter „Lebensereignisse“ Informationen über deine religiösen Ansichten, deine politischen Einstellungen oder deine Gesundheit bzw. an wem du „interessiert“ bist angeben. Diese und andere Informationen (wie etwa Nationalität oder ethnische Herkunft, weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit) unterliegen nach EU-Recht einem besonderen Schutz.

- Netzwerke und Verbindungen.** Wir erfassen Informationen über die Personen, [Seiten](#), [Konten](#), [Hashtags](#) und Gruppen, mit denen du verbunden bist und darüber, wie du mit ihnen in unseren Produkten

Bereitgestellte Informationen genügen rechtl. Anforderungen, erfüllen aber ihren Zweck nicht

→ Neue, weniger „dysfunktionale“ Ansätze notwendig

Von der Datenschutzerklärung zu neuen Präsentationsformen

DaSKITA

Hinweis zu ausgelagerten Dienstleistungen: Bestimmte Drittanbieter und Unternehmen der PayPal-Gruppe erbringen Dienstleistungen für PayPal (Europe) S.à.r.l. et Cie, S.à.r.l. (PayPal), damit PayPal ihre Dienstleistungen anbieten kann. Wir geben möglicherweise Daten zu diesen Personen weiter. Aus dieser central disclosure werden wir Ihre persönlichen vollständig persönlichen Angaben und Einzelheiten zu Ihren Transaktionen. Diese Drittanbieter haben Ihre Sitz in verschiedenen Orten in der Europäischen Union (insbesondere Frankreich, Deutschland, Italien, Spanien, Niederlande, Belgien, Italien, Polen, Spanien, Schweden, Dänemark) und dem Vereinigten Königreich sowie in Tansania, Ägypten, Schottland, die Philippinen und den Vereinigten Staaten. Gemäß dem Luxemburger Gesetz über den Finanzsektor haben wir diese Liste geändert, um die für solche Übertragungen erforderlichen Daten zu beinhalten.

Kategorie	Name der Partei und Geschäftszweck (in Klammern)	Zweck	Offengelegte Daten
1. Zahlungsdienstleistungen	Banken Bank PLC (GB), HSBC Bank PLC (GB), Citibank, Citibank Merchant Services LLP (USA), Bank of America N.A. (USA), CIBC, BA Commerce Italia, Phoenix Limited (Ireland), Citicore Financial Services (USA), (Paying) Chase Bank (USA), BNP Paribas (Frankreich), Ingenio (Schweiz), Wells Fargo (USA), American Express (USA), National Westminster Bank PLC (GB), Citigroup Limited (Ireland), Australia and New Zealand Banking Group Limited (Neuseeland), ANZ National Bank Limited (Neuseeland), Transaction Network Services UK Limited (GB)	Zahlungserstellung, Abwicklungsdienste und Betrugserkennung	Name, Adresse, E-Mail-Adresse, Telefonnummer, Angaben zu Zahlungsguthaben des Nutzers und Angaben zu Zahlungstransaktionen, Kontennummernnummern.
	BNP Paribas (Frankreich)	Zahlungserstellung, Betrugserkennung und Aufbuchung der Transaktionen von PayPal-Nutzern, wenn diese mit einem Konto zu tun haben, das der PayPal-Dienst über den	Name, E-Mail-Adresse, Telefonnummer, Adresse, IP-Adresse, Gebietskürzel, PayPal-Kontennummer, Einheiten zu den Transaktionskonten des Nutzers und Angaben zu Zahlungstransaktionen.
		Öffnen und lesen über den	Name, Adresse, E-Mail-Adresse, Telefonnummer, Angaben zu den Transaktionskonten des Nutzers und anderen Angaben zu Zahlungstransaktionen.
		Geld-	Name, Transaktionsnummer und -betrag, Währung und Selbstbeschreibung des Nutzers.
		Verfügen vom	Alle Konteninformationen über Details zu Transaktionskonten des Nutzers.

Welche Arten von Informationen erfassen wir?

Zur Bereitstellung der Facebook-Produkte müssen wir Informationen über dich verarbeiten. Die Arten der von uns erfassten Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, wie du auf von uns erfasste Informationen zugreifen bzw. sie löschen kannst, indem du die Facebook-Einstellungen beim die Instagram-Einstellungen besuchst.

- Von dir und anderen geteilte und bereitgestellte Dinge.
 - Von dir bereitgestellte Informationen und Inhalte. Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt, das gehören auch deine Registrierungen für ein Konto, die Erstellen oder Teilen von Inhalten sowie der Nachrichtenaustausch bzw. die Kommunikationen mit anderen. Das kann Informationen über die von dir bereitgestellten Inhalte oder solche, die in ihnen enthalten sind (wie Metadaten) umfassen, wie z.B. den Aufnahmezeitpunkt eines Fotos oder das Datum, an dem eine Datei erstellt wurde. Es kann auch das umfassen, was du durch von uns bereitgestellte Funktionen, wie z.B. unsere Karten, siehst, damit wir dir personalisierte Medien und Filter, die dir gefallen könnten, vorschlagen oder dir Tipps für die Verwendung des Hochformats geben können. Unsere Systeme verarbeiten von dir bereitgestellte Inhalte und Mitteilungen automatisch, um den Kontext und die in ihnen enthaltenen Details für die unten beschriebenen Zwecke zu analysieren. Erfahre mehr darüber, wie du kontrollieren kannst, wer die Dinge sehen kann, die du teilst.
 - Daten mit besonderem Schutz. Du kannst in deinen Facebook-Einstellungen oder unter „Lebensereignisse“ Informationen über deine religiösen Ansichten, deine politischen Einstellungen oder deine Gesundheit bzw. an wem du „intimes“ teilst eingeben. Diese und andere Informationen (wie eine Nationalität oder ethnische Herkunft, weltanschauliche Überzeugungen oder eine Gewerkschaftsangehörigkeit) unterliegen nach EU-Recht einem besonderen Schutz.
 - Netzwerke und Verbindungen. Wir erfassen Informationen über die Personen, Seiten, Konten, Hashtags und Gruppen, mit denen du wechselst, bist und darüber, wie du mit ihnen interagierst.



Controller: Green Company AG
Data Protection Officer: Jane Super
Data Disclosed (#): 1
Automated Decision Making: in use
Third country Transfers:

Learn more

Browser-Plugins



Visualisierung von Weitergabernetzwerken



TYPE OF DATA COLLECTED	GENERAL DATA PRACTICES	DATA SHARING
Personal: Name, mailing address, email, or phone number	Not automated: Data is not used for automated decision making or advertising	Affiliates: Affiliates and subsidiaries processing the same privacy practices
Corporate: All data is stored in a secure system	Data portability: We allow you to export your data to your own system or to another service	Contractors: Third party contractors to provide services to us may have access to your data
Information: We collect information about your behavior or search history	Public display: We allow users to share information publicly on our website	Third parties: Third parties may have access to your data
Financial: We collect status or activity information or purchase history	User control: Users are allowed to access and control personal information	
Personal: We collect personal information, such as documents or media	Data retention: We retain data for as long as it is needed for business purposes	

Privacy Icons

Von der Datenschutzerklärung zu neuen Präsentationsformen

DaSKITA

Welche Arten von Informationen erfassen wir?

Zur Bereitstellung der Produkt-Funktionen müssen wir Informationen über dich verarbeiten. Die Art und der Umfang der Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.

Von dir und anderen geteilte und bereitgestellte Dinge:

- **Von dir bereitgestellte Informationen und Inhalte:** Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt. Das können auch deine Registrierungs- oder andere Identifikationsdaten sein, die du uns mitteilen wirst. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.
- **Informationen, die wir von anderen erhalten:** Wir erfassen Informationen, die wir von anderen erhalten, wenn du unsere Produkte nutzt. Das können auch deine Registrierungs- oder andere Identifikationsdaten sein, die du uns mitteilen wirst. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.

Welche Arten von Informationen erfassen wir?

Zur Bereitstellung der Produkt-Funktionen müssen wir Informationen über dich verarbeiten. Die Art und der Umfang der Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.

Von dir und anderen geteilte und bereitgestellte Dinge:

- **Von dir bereitgestellte Informationen und Inhalte:** Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt. Das können auch deine Registrierungs- oder andere Identifikationsdaten sein, die du uns mitteilen wirst. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.
- **Informationen, die wir von anderen erhalten:** Wir erfassen Informationen, die wir von anderen erhalten, wenn du unsere Produkte nutzt. Das können auch deine Registrierungs- oder andere Identifikationsdaten sein, die du uns mitteilen wirst. Du kannst erfahren, was du auf wir von uns erfassene Informationen angucken bzw. sie löschen kannst, wenn du die Datenschutz-Einstellungen bzw. die datenschutzrechtlichen Hinweise betrachtest.

Transparency Information Language & Toolkit

```

15  "controller": {
    "name": "Green Company AG",
    "division": "Product line e-mobility",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "representative": {
      "name": "Jane Super",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    }
  },
20  "dataProtectionOfficer": {
    "name": "Jane Super",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "email": "contact@greencompany.de",
    "phone": "0049 151 1234 5678"
  },
25  "dataDisclosed": {
    "id": "f1424f86-ca0f-4f0c-9438-43cc00509931",
    "category": "E-mail address",
  },
35  "data": {
    "id": "f1424f86-ca0f-4f0c-9438-43cc00509931",
    "category": "E-mail address",
  }
  
```

Controller: Green Company AG
 Data Protection Officer: Jane Super
 Data Disclosed (#): 1
 Automated Decision Making: In use
 Third country Transfers: DE, FR

Learn more

Browser-Plugins



Visualisierung von Weitergabernetzwerken

TYPE OF DATA COLLECTED	SEVERAL DATA PRACTICES	DATA SHARING
- Location - Device - Usage - Identity - Interactions - Device - Usage - Identity - Interactions	- Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting	- Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting - Ad targeting

Privacy Icons



Formale, maschinenlesbare Repräsentation von Transparenzangaben (Art. 12ff DSGVO)

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

DSGVO-Anforderungen



Reference(s)	Transparency information
13 (1a) 14 (1a) 30 (1a)	Controller
13 (1b) 14 (1b) 30 (1a)	Data protection officer
13 (1c) 14 (1c) 15 (1a) 30 (1b)	Purposes
13 (1c) 14 (1c)	Legal basis
13 (1d) 14 (2b)	Legitimate interests
13 (1e) 14 (1e) 15 (1c) 30 (1d)	Recipient (categories)
13 (1f) 14 (1f) 15 (1c) 30 (1e)	Third country transfer
13 (1f) 14 (1f) 15 (2) 30 (1e)	Adequacy (third country)
13 (1f) 14 (1f) 15 (2) 30 (1e)	Access and Data portability
13 (2a) 14 (2a) 15 (1d) 30 (1f)	Retention or storage criteria

Kategorisierung



Meta	Access/Data portability
1. Identification Number ⁴	1. Possibility available ⁷
2. Name ⁶	2. Description accessibility
3. Creation date ⁶	3. URL
4. Modification date ⁶	4. E-mail
5. Version ⁶	5. [Identification evidence]
6. Language code ⁴	6. Administrative fee
7. Status ⁶	a. Amount b. Currency
8. URL ⁶	7. Data format(s)
9. Hash ⁴	
Controller	Sources¹², per item:
1. Company name ⁶	1. Data (category)
2. Division ⁷	2. [Sources]
3. Address ⁶	a. Description
4. Country code ⁴	b. URL
5. Name (representative) ⁶	c. Publicly available?
6. Email (representative) ⁶	
7. Phone (representative) ⁶	Rights to information, rectification/deletion, data portability

Detailanalyse notw. Ausdrucksmächtigkeit



```

dataDisclosed := ((
65  id,
    category,
    purposes,
    legalBases,
    legitimateInterests,
    (recipients | category),
    storage,
    nonDisclosure,
    [addProp]
70  ));
    
```

Formale Sprachspezifikation

Formale, maschinenlesbare Repr.



```

"controller": {
  "name": "Green Company AG",
  "division": "Product line e-mobility",
  "address": "Wolfsburger Ring 2, 38440 Berlin",
  "country": "DE",
  "representative": {
    "name": "Jane Super",
    "email": "contact@greencompany.de",
    "phone": "0049 151 1234 5678"
  }
},
"dataProtectionOfficer": {
  "name": "Jane Super",
  "address": "Wolfsburger Ring 2, 38440 Berlin",
  "country": "DE",
  "email": "contact@greencompany.de",
  "phone": "0049 151 1234 5678"
},
"dataDisclosed": [
  {
    "_id": "f1424f56-ca0f-4f0c-9438-43cc0809931",
    "category": "E-mail address",
    "purpose": {
35  [
    ]
  }
}
]
    
```



TILT: A GDPR-Aligned Transparency Information Language and Toolkit for Practical Privacy Engineering

Elias Grünewald
Technische Universität Berlin
Information Systems Engineering Research Group
Berlin, Germany
gruenewald@tu-berlin.de

Frank Pallas
Technische Universität Berlin
Information Systems Engineering Research Group
Berlin, Germany
frank.pallas@tu-berlin.de

ABSTRACT

In this paper, we present TILT, a transparency information language and toolkit explicitly designed to represent and process transparency information in line with the requirements of the GDPR and allowing for a more automated and adaptive use of such information than established, legalese data protection policies do.

We provide a detailed analysis of transparency obligations from the GDPR to identify the expressiveness required for a formal transparency language intended to meet respective legal requirements. In addition, we identify a set of further, non-functional requirements that need to be met to foster practical adoption in real-world (web) information systems engineering. On this basis, we specify our formal language and present a respective, fully implemented toolkit around it. We then evaluate the practical applicability of our language and toolkit and demonstrate the additional prospects it unlocks through two different use cases: *a)* the inter-organizational analysis of personal data-related practices allowing, for instance, to uncover data sharing networks based on explicitly announced transparency information and *b)* the presentation of formally represented transparency information to users through novel, more comprehensible, and potentially adaptive user interfaces, heightening data subjects' actual informedness about data-related practices and, thus, their sovereignty.

Altogether, our transparency information language and toolkit allow - differently from previous work - to express transparency information in line with actual legal requirements and practices of modern (web) information systems engineering and thereby pave the way for a multitude of novel possibilities to heighten transparency and user sovereignty in practice.

CCS CONCEPTS

• Applied computing → Law, Information systems → Information systems applications: Web data description languages; • Software and its engineering → Formal language definitions; Context specific languages; • Security and privacy → Privacy protections.

KEYWORDS

Data transparency, GDPR, data protection, privacy by design, legal informatics, privacy engineering

1 INTRODUCTION

Transparency has been a core principle in philosophical, legal, and technical deliberations around privacy¹ for decades. This particularly applies to data privacy in everyday digital life: To be able to act in a sovereign and self-determined way and actually make informed choices, individuals need to have sufficient knowledge about the actual facts and given regarding the processing of personal data, including, e.g., which party collects what personal data for which purposes, how long this data is (going to be) stored, et cetera. Data protection laws and regulations around the world - such as the European General Data Protection Regulation (GDPR) [8] or the California Consumer Privacy Act (CCPA) [36] - therefore explicitly include transparency rules for data processing parties, obligating them to reveal respective information to the data subjects.

These obligations are today typically fulfilled through respective transparency parts of written privacy policies. Such privacy policies do, however, exhibit several shortcomings that severely limit their actual reception and comprehension on the side of data subjects: First of all, privacy policies are often long, complex, and written in legalese language, making it hard for data subjects to locate transparency-related information and actually understand them correctly [24, 33]. Second, different privacy policies employ different logical structures and vocabularies for factually similar statements, causing significant reading and decoding efforts for every new policy to be understood [25]. Such practice structurally discriminates people who are less privacy-literate [37]. Finally, data transfers towards other parties are now a broadly established practice. Data subjects wanting to see "the whole picture" in such contexts therefore have to read and understand multiple policies and establish the logical interdependencies between them themselves.

Together with the ever-increasing number of services used (and, thus, of privacy policies to be read), this leads to a state where privacy policies, including respective transparency statements, are not read anymore before using a particular service and/or consenting to a certain collection and use of personal data [27]. Under such conditions, transparency statements increasingly degenerate into rather self-serving formal compliance exercises instead of actually fostering data subjects' informedness of decisions and self-sovereign conduct with regard to privacy.

For other areas of privacy, dedicated technologies have repeatedly been demonstrated to be capable of lowering the cognitive and administrative effort required on the side of data subjects and thereby of re-aligning the actual real-world practice to the (still

¹Using well aware of the slightly different notions between "Privacy" and "Data Protection", we use these terms interchangeably herein.

ACM FAccT 2021

DaSKITA



```

15  *controller*: {
    "name": "Green Company AG",
    "division": "Product line e-mobility",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "representative": {
      "name": "Jane Super",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    }
  },
  *dataProtectionOfficer*: {
25    "name": "Jane Super",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "email": "contact@greencompany.de",
    "phone": "0049 151 1234 5678"
  },
30  *dataDisclosed*: {
    "_id": "f1424f86-ca0f-4f0c-9438-430c00509931",
    "category": "E-mail address",
35  }

```

Visualisierung von Weitergabernetzwerken

Privacy Icons

→ @eliasgruenewald

<addendum>

Von der Datenschutzerklärung zur strukturierten Repräsentation

DaSKITA

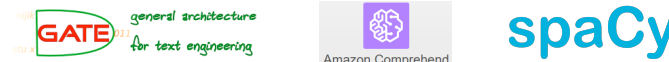
Welche Arten von Informationen erfassen wir?

Zur Bearbeitung der Produkt-Anfragen müssen wir Informationen über dich verarbeiten. Die Arten der von uns erfassten Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, wie du auf wir uns erfassten Informationen angucken bzw. wie du sie löschen kannst, indem du die Datenschutz-Einstellungen bzw. die zugehörigen Einstellungen betrachtest.

Von dir und anderen geteilte und bereitgestellte Dinge:

- **Von dir bereitgestellte Informationen und Inhalte:** Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt, das gilt auch für deine Registrierung für ein Konto, das Erstellen oder Teilen von Inhalten sowie der Nachrichtenversand bzw. die Kommunikation mit anderen. Das kann Informationen über die von dir bereitgestellten Inhalte oder solche, die in einer Mitteilung oder einer Mitteilung enthalten sind, wie z.B. die Aufnahme eines Fotos oder das Datum, an dem eine Datei erstellt wurde. Es kann auch sein, dass du uns mitteilen, wie du dich bei unseren Produkten verhältst, wie z.B. unsere Namen, wenn du dich bei unseren Produkten registrierst oder die Typen für die Verwendung des Hochformats geben können. Unsere Systeme verarbeiten von dir bereitgestellte Inhalte und Metadaten automatisch, um den Kontext und die in ihnen enthaltenen Details für die gegen beschriebenen Zwecke zu analysieren. Erfahre mehr darüber, wie du kontrollieren kannst, was die Dinge sehen kann, die du teilst.
- **Informen wir besonderen Schutz:** Du kannst in deinen Produkt-Einstellungen oder unter „Datenschutz“ Informationen über deine registrierten Accounts, deine persönlichen Einstellungen oder deine Gewissheit bzw. an wen du „passiviert“ bist anzeigen. Diese und andere Informationen bieten insbesondere eine ethische Herkunft, verhaltensbasierte Überlegungen oder eine Zweckbindung (z.B. für den Kontakt) vor. Wir werden diese Informationen (z.B. für den Kontakt) vor. Wir werden diese Informationen (z.B. für den Kontakt) vor.
- **Netzwerke und Verbindungen:** Wir erfassen Informationen über die Netzwerk-Adressen, Namen, Zugangsdaten und Gruppen, mit denen du verbunden bist und darüber, wie du mit diesen in unseren Produkten interagierst.

Extraktion: KI-basierte Verfahren des Natural Language Processing (NLP)



+ Implementierungsnaher Annotation:
Neue Mechanismen zur Hinterlegung von
Transparenzinformationen im Programmcode

+ Web-basiertes Annotationstool zur kollaborativen,
manuellen Überführung

Transparency Information Language & Toolkit

```

15  *controller*: {
    "name": "Green Company AG",
    "division": "Product line e-mobility",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "representative": {
      "name": "Jane Super",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    }
  },
20  *dataProtectionOfficer*: {
    "name": "Jane Super",
    "address": "Wolfsburger Ring 2, 38440 Berlin",
    "country": "DE",
    "email": "contact@greencompany.de",
    "phone": "0049 151 1234 5678"
  },
25  *dataDisclosed*: {
    "id": "f1424f86-ca0f-4f0e-9438-43ee00509931",
    "category": "E-mail address",
  },
30  },
35  }
  
```

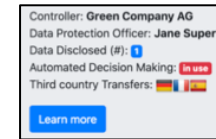
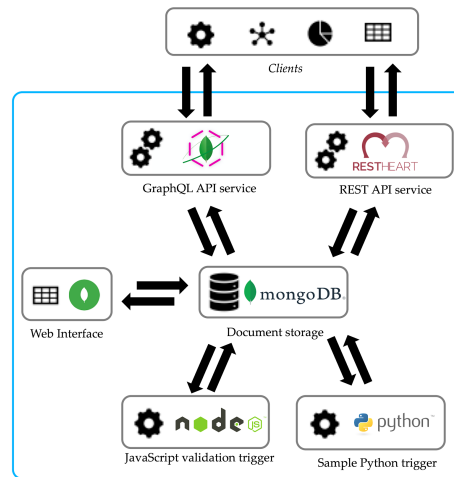
Von der Datenschutzerklärung zu neuen Präsentationsformen

Transparency Information Language & Toolkit

```
15 *controller*: {  
  "name": "Green Company AG",  
  "division": "Product line e-mobility",  
  "address": "Wolfsburger Ring 2, 38440 Berlin",  
  "country": "DE",  
  "representative": {  
    "name": "Jane Super",  
    "email": "contact@greencompany.de",  
    "phone": "0049 151 1234 5678"  
  }  
},  
20 *dataProtectionOfficer*: {  
  "name": "Jane Super",  
  "address": "Wolfsburger Ring 2, 38440 Berlin",  
  "country": "DE",  
  "email": "contact@greencompany.de",  
  "phone": "0049 151 1234 5678"  
},  
25 *dataDisclosed*: {  
  "_id": "f1424f86-ca0f-4f0c-9438-43ce00509931",  
  "category": "E-mail address",  
}
```



Ablage-, Abfrage- und Abanalysplattform



Browser-Plugins



Visualisierung von Weitergabernetzwerken

TYPE OF DATA COLLECTED	SEVERAL DATA PRACTICES	DATA SHARING
Location data (e.g., IP address, GPS data)	Data retention (e.g., storing data for a long time)	Data sharing (e.g., sharing data with third parties)
Personal data (e.g., name, email, phone number)	Data processing (e.g., analyzing data, creating profiles)	Data transfer (e.g., transferring data to other systems)
Sensitive data (e.g., health data, financial data)	Data security (e.g., protecting data from unauthorized access)	Data deletion (e.g., deleting data when no longer needed)
Metadata (e.g., data about data)	Data access (e.g., controlling who can access data)	Data anonymization (e.g., removing personally identifiable information)
Cookies (e.g., tracking user behavior)	Data backup (e.g., creating copies of data for recovery)	Data portability (e.g., allowing users to move their data to another service)
Biometric data (e.g., fingerprints, facial recognition)	Data integration (e.g., combining data from different sources)	Data archiving (e.g., storing data for long-term preservation)
Financial data (e.g., bank accounts, credit cards)	Data monitoring (e.g., watching data usage and security)	Data encryption (e.g., protecting data with codes)
Health data (e.g., medical records, fitness data)	Data testing (e.g., checking data for errors and quality)	Data governance (e.g., managing data quality and security)
Social media data (e.g., posts, comments, likes)	Data audit (e.g., reviewing data handling processes)	Data compliance (e.g., ensuring data handling follows laws and regulations)

Privacy Icons

</addendum>